Julio de 2014

Aplicaciones seguras para un entorno Cloud más confiable

Refuerce la protección de las aplicaciones —del diseño a la implementación— para abordar activamente los riesgos en la seguridad Cloud



Introducción

Por su frecuente cobertura en los medios, los incidentes de seguridad de Internet se han vuelto un tema de conversación popular. Naturalmente, los comentarios sobre el riesgo de seguridad se extienden también a la nube. En un informe reciente sobre el uso de la computación en nube, el 65% de las organizaciones encuestadas mencionaron la seguridad como su principal obstáculo en la adopción Cloud.[1]

Lamentablemente, muchas organizaciones no advierten que la infraestructura Cloud en realidad les ofrece una oportunidad única de mejorar la seguridad. De hecho, la seguridad Cloud puede ser más automatizada, personalizable y elástica que las tradicionales defensas perimetrales y los productos puntuales y estáticos. Las organizaciones que implementan aplicaciones con base en la nube tienen la oportunidad de mejorar las mejores prácticas y políticas usadas para asegurar sus infraestructuras de TI tradicionales. En suma, la computación en nube puedeser segura.

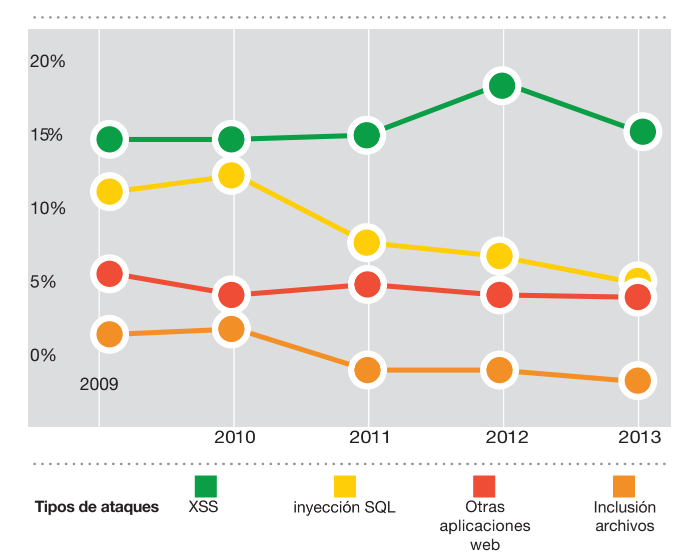
Proteger las aplicaciones de las vulnerabilidades de seguridad es vital para mejorar la postura de seguridad de una organización, tanto en el ámbito tradicional (on-premise) como en la nube. Los informes IBM® X-Force® mostraron que las aplicaciones siguen siendo un punto atractivo de entrada para el ataque. En 2013, los atacantes explotaron con éxito aplicaciones web vulnerables con ataques del tipo inyección SQL (SQLi) y cross-site scripting (XSS), al tiempo que usaron una combinación de herramientas sofisticadas y generalmente accesibles para abrirse paso.[2] Estas violaciones de seguridad pueden tener un impacto financiero significativo en términos de penalidades, daño a la propiedad intelectual, pérdida de confianza de los clientes y pérdida de capital.

Este documento analiza cómo un programa eficaz de seguridad de aplicaciones puede ayudar a las organizaciones a proteger sus invalorables activos de datos digitales en la nube. También explica cómo enfoque de seguridad de las aplicaciones que es seguro por diseñopuede contribuir a reducir el riesgo general en toda la infraestructura informática, en la nube y más allá.

Riesgos (y oportunidades) de la seguridad Cloud

¿Por qué es tan vital la seguridad de aplicaciones en un entorno Cloud? Porque los atacantes sofisticados de hoy están creando malware más inteligente. Trabajando desde aplicaciones infectadas, el malware puede buscar vulnerabilidades en otras aplicaciones en un punto terminal, en general relacionado con aplicaciones empresariales propietarias que el atacante antes no había accedido. Cuando ubica una vulnerabilidad, el malware puede explotarla para tener acceso sin precedentes a datos valiosos y sensibles.

La seguridad Cloud también está estrechamente conectada con la seguridad de aplicaciones web. Conforme crece la cantidad de datos de organizaciones que se almacenan y acceden en la nube, los hackers están más motivados que nunca para irrumpir en sitios y aplicaciones web que acceden a datos de alto valor. La investigación realizada por X-Force muestra que los atacantes siguen usando tácticas de explotación SQLi y XSS en grandes cantidades, lo cual indica que muchos sistemas legados y otras aplicaciones web sin parches siguen siendo vulnerables.[2] No proteger datos en tránsito a y de una aplicación web puede ocasionar filtración de datos sobre credenciales de usuario, tarjetas de crédito y comunicaciones privadas en apariencia.



Pero la realidad no tiene por qué ser tan gris y desalentadora. Las características de la arquitectura Cloud – como estandarización, automatización de la carga de trabajo, recursos virtualizados y mayor visibilidad de infraestructura – pueden mejorar sustancialmente los niveles de seguridad para la mayoría de las organizaciones.

Utilizando un conjunto definido de interfaces Cloud, junto con políticas de control centralizado de identidades y accesos, las organizaciones pueden ayudar a reducir el riesgo de que usuarios no autorizados accedan a recursos a los que no deberían acceder. Ejecutar los servicios de cómputo en dominios aislados, proporcionar cifrado de datos como estándar en movimiento y en descanso, y controlar los datos a través del almacenamiento virtual son medidas que pueden mejorar la rendición de cuentas y reducir la pérdida potencial de datos. Además, el aprovisionamiento automatizado puede contribuir a reducir los ataques y a mejorar la investigación.

Pasos claves para administrar la seguridad de aplicaciones en Cloud

Muchas organizaciones utilizan aplicaciones de software diseñadas in-house para ejecutar procesos de negocio críticos, realizar transacciones con proveedores y entregar servicios sofisticados a los clientes. Asegurar estas aplicaciones rara vez es una prioridad. Pero debería serlo. Porque en el panorama de amenazas cada vez más sofisticadas de la actualidad –en el que los atacantes encuentran nuevas formas de desestabilizar aplicaciones y obtienen acceso irrestricto a datos confidenciales – las organizaciones deben adoptar una estrategia integral para la seguridad de las aplicaciones.

Para combatir la amenaza creciente de violaciones de seguridad en la nube, es importante abordar los siguientes pasos claves:

- **Establezca su postura de riesgo.** Evalúe cómo su postura de seguridad se compara con el panorama de amenazas internas y externas. Las soluciones de inteligencia de seguridad pueden ayudar a su organización a controlar continuamente el entorno, colocar vulnerabilidades en contexto y mantener una visión en tiempo real de su postura de riesgo.

- **Proteja sus datos.** La seguridad de los datos es un proceso contínuo, que incluye entender dónde residen los datos sensibles, quién los usa y con qué frecuencia, y bloquear el acceso no autorizado. La tecnología de supervisión de actividad de datos puede ofrecer visibilidad del acceso de datos, ya sea que los datos estén ubicados en bases de datos estructuradas, sistemas no estructurados o plataformas big data. Esto puede ayudar a mejorar la seguridad de la información en entornos tradicionales y de nube.

- **Conozca a su usuario.** Además de verificar las identidades de usuarios, las organizaciones deben controlar a qué acceden los usuarios y en qué contexto. Las soluciones de administración de identidades federadas pueden ayudar a proteger y autenticar el acceso de usuarios a aplicaciones Cloud y software-as-a-service (SaaS).

- **Incorpore seguridad de aplicaciones al ciclo de vida de desarrollo de software.** Cada vez más, los atacantes explotan vulnerabilidades para bajar malware a puntos terminales de los usuarios desprevenidos. Escanear las aplicaciones y probar que no tengan vulnerabilidades como parte del desarrollo de aplicaciones –así como en producción – es esencial para mantener un entorno seguro.

- **Protéjase de amenazas y fraude.** La protección integral de amenazas sigue siendo importante para la nube. Los atacantes pueden seguir infiltrándose en las redes y acceder a bases de datos privilegiadas, cometiendo fraude. Una combinación eficaz de productos de seguridad de red, analítica de seguridad e inteligencia de amenazas puede ayudar a las organizaciones a mitigar las amenazas y prevenir el fraude.

En las noticias: El costo de una violación de la seguridad

Las aplicaciones con seguridad insuficiente pueden tener consecuencias nefastas. Un informe reciente señaló que el costo total promedio de una violación de datos empresarial es ahora de USD5.85 millones, y los incidentes podrían costar tanto como USD246 por registro comprometido.[3]

Seguridad incorporada al diseño, no agregada

En otras épocas, la seguridad era considerada un problema de TI, no un problema de desarrollo. Pero en la actualidad, los expertos en seguridad se dieron cuenta de que la protección empieza al nivel del código. Y al encontrar y remediar vulnerabilidades de seguridad en el ciclo de vida de desarrollo, las organizaciones pueden ahorrar enormes cantidades de dinero. De hecho, el IBM Systems Science Institute concluyó que puede ser hasta 100 veces más caro solucionar defectos en el ambiente de producción que hacerlo durante el desarrollo.[4]

La seguridad de aplicaciones principio a fin, del diseño a la implementació



Con un enfoque de seguridad de aplicaciones que es "seguro por diseño", las organizaciones pueden abordar las vulnerabilidades al inicio del proceso de desarrollo. Las prácticas de código seguro forman parte del diseño de aplicaciones, en lugar de dejar la seguridad para el final. Para garantizar la seguridad de sus aplicaciones en la nube, las organizaciones deben:

- Escanear aplicaciones. Al escanear el código fuente de las aplicaciones como parte del ciclo de vida de desarrollo, la organización puede resolver los problemas de seguridad a medida que se presentan. Esto puede contribuir a ahorrar tiempo y reducir costos. Las soluciones de prueba de aplicaciones también pueden ayudar a entrenar a los desarrolladores al proporcionar información detallada sobre defectos crónicos y amenazas de seguridad emergentes.
- **Clasificar y validar aplicaciones.** Para comprender la postura de riesgo de aplicaciones implementadas, la organización puede realizar escaneos dinámicos de aplicaciones en el tiempo de ejecución. Esto permite a las organizaciones evaluar la seguridad de las aplicaciones de producción y validar la eficacia de las medidas correctivas.
- **Implementar aplicaciones con seguridad.** Las organizaciones pueden proteger datos sensibles implementando aplicaciones Cloud, Web y Móviles con una visión informada del riesgo. Además de la prueba de penetración manual, las herramientas automatizadas pueden proporcionar un análisis coherente, confiable y escalable de las vulnerabilidades de seguridad de aplicaciones. Al integrarse con inteligencia de amenazas actualizada, las organizaciones también pueden priorizar esfuerzos de remediación sobre la base del riesgo potencial.

Además de los escaneos continuos de seguridad de aplicaciones – para ayudar a identificar vulnerabilidades cuando se implementan nuevas funcionalidades o se aplican parches – las organizaciones también necesitan poder responder al contexto de red de las vulnerabilidades de aplicaciones. Deben poder correlacionar comportamientos inusuales en todo el entorno, detectando proactivamente filtraciones de datos, reconociendo cuando la información está siendo enviada a ubicaciones no autorizadas e impidiendo los ataques de malware antes de que puedan robar información valiosa.

Las defensas perimetrales, como firewalls y sistemas de prevención de intrusiones, son un complemento importante de las soluciones de prueba de seguridad de las aplicaciones. Las organizaciones pueden combinar la funcionalidad de análisis de red con información sobre vulnerabilidades de aplicaciones e identificar si hay vulnerabilidades que están siendo activamente explotadas.

Tranquilidad para entornos Cloud de todos los tamaños

IBM puede ayudar a las organizaciones a desarrollar una visión integral de la seguridad en la nube. Con escalabilidad fácil para dar soporte incluso a entornos de nube muy grandes, las soluciones IBM Security proporcionan protección por capas y conocimientos profundos en toda la infraestructura. Capacidades tales como single-sign-on federado y administración de usuarios privilegiados ayudan a proporcionar acceso y control simplificados en múltiples servicios de nube para potencialmente millones de usuarios. La supervisión de bases de datos y escaneo de aplicaciones web y móviles ayudan a reducir las vulnerabilidades de datos y aplicaciones. Las soluciones IBM también dan soporte al cumplimiento de seguridad con administración de parches para puntos terminales y máquinas virtualizadas. Y lo que es más, estas soluciones aumentan la visibilidad y mejoran la auditoría de la actividad de nube dentro de entornos multi-tenant.

Las soluciones, como IBM Security QRadar® SIEM y las soluciones de prevención de intrusiones en la red de IBM Security, ofrecen protección adicional para cargas de trabajo Cloud y usuarios Cloud. Al controlar todo el tráfico que entra y sale de la nube, o el tráfico dentro de la nube, las soluciones IBM Security QRadar pueden correlacionar vulnerabilidades conocidas de aplicaciones con otros eventos y alertas, y permitir a las organizaciones administrar en forma preventiva los riesgos y establecer prioridades para las acciones correctivas. Las soluciones de prevención de intrusiones de red de IBM Security también pueden ayudar a proteger contra adjuntos maliciosos, ataques de denegación de servicio, pérdida de datos y ataques enfocados, relacionados con amenazas persistentes avanzadas.

Conclusión

La seguridad integral de aplicaciones –y una cultura segura por diseño- forma parte de una seguridad de nube eficaz. Los atacantes son cada vez más adeptos a encontrar vulnerabilidades de aplicaciones y usarlas para obtener acceso a datos de alto valor almacenados en bases de datos corporativas de back-end. Pero gracias al control y escaneo continuo de las aplicaciones, las organizaciones pueden protegerse de las vulnerabilidades y ayudar a detener las amenazas antes de que impacten en el negocio.

Para ver más información sobre otras ofertas IBM Security, visite:**http://www-03.ibm.com/**security/ar/es/
ibm.com/financing

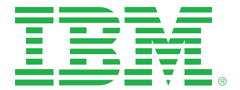
Para conocer más sobre cómo mejorar sus posturas de seguridad de seguridad de aplicaciones, baje el white paper IBM " Five critical steps to achieving an effective application security program " (Cinco pasos críticos para alcanzar un programa de seguridad de aplicaciones eficaz).

Además, IBM Global Financing puede ayudarlo a adquirir las capacidades de software que su empresa necesita en la forma más económica y estratégica posible. Trabajamos con clientes con calificación crediticia para personalizar una solución de financiación que se adapte a las características y objetivos de desarrollo de su empresa, permita una administración eficaz del efectivo y mejore el costo total de propiedad. Financie su inversión crítica en TI e impulse su negocio hacia adelante con IBM Global Financing. Más información: **ibm.com**/financing

Si quiere que un especialista de IBM lo contacte, **haga click aquí** y complete sus datos.

[3] "2014 Cost of Data Breach Study: Global Analysis," P*onemon Institute with IBM*, mayo de 2014. **ibm.com**/services/costofbreach

[4] Mano Paul, "The Need for Secure Software," *ISC2*, *Software Magazine*, 20 de marzo de 2014. http://www.softwaremag.com/DSN/wwwswmagcom/Content/ClientAssets/ISC_WPaper_03-20-14.pdf



IBM Corporation
Software Group
Route 100
Somers, NY 10589

Producido en Estados Unidos de América
Julio de 2014

[1] Terri Eyden y Jason Bramwell, "Survey Provides Insight into Cloud Computing Usage," Accounting WEB, 25 de septiembre de 2013. http://www.accountingweb.com/article/survey-provides-insight-cloud-computing-usage/222453

[2] IBM X-Force, "IBM X-Force Threat Intelligence Quarterly - 1Q 2014," febrero de 2014. https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-WW_Security_Organic&S_PKG=ov21294&S_TACT=102PW99W

